УДК 338.47:65.012.8

Віктор Данчук, доктор фізико-математичних наук, професор (завідуючий кафедрою «Електроніка та обчислювальна техніка», Національний транспортний університет)

Віталій Гурнак, доктор економічних наук
(професор кафедри «Транспортне право і логістика», Національний транспортний університет)

Олексій Ананченко
(магістр, Національний транспортний університет)

Віталій Ананченко,
(магістр, Державний університет телекомунікацій)

КОМПЛЕКСНЕ ЗАСТОСУВАННЯ ПІДПРИЄМСТВАМИ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІКО-ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ

У статті висвітлюється роль, значення і специфіка комплексного застосування методів щодо інформаційної безпеки телекомунікаційних мереж загального користування в галузях промисловості, торгівлі, транспорту та зв'язку. Показано шляхи взаємодії корпоративних мереж з телекомунікаційними мережами загального користування. Проаналізовано можливості корпоративної інформаційної системи «Наука в університетах», розробленої Національним транспортним університетом та впровадженої в практику Міністерством освіти і науки України. Обґрунтовується, що інформаційна безпека, як і захист інформації, є завданням комплексним, спрямованим на забезпечення безпеки та реалізується впровадженням різноманітних систем безпеки. В статті сформульовано три базові принципи, які повинна забезпечувати інформаційна безпека: цілісність даних – захист від збоїв, що ведуть до втрати інформації, захист від неавторизованого створення та знищення даних; конфіденційність інформації; доступність інформації для всіх авторизованих користувачів. Дослідженням встановлено, що підтримка інформаційної безпеки – це комплекс організаційних, правових та інженерно-технологічних заходів щодо збереження, охорони та захисту життєво важливих інтересів суб'єктів інформаційної діяльності. Інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства) – це суспільні відносини щодо створення та підтримання на усвідомленому, належному рівні функціонування відповідної автоматизованої (комп'ютеризованої) інформаційної системи.

***Ключові слова**: інформаційна безпека, телекомунікаційні мережі, корпоративні мережі, інформатизація, інформаційна система, захист інформації.*

Виктор Данчук, доктор физико-математических наук, профессор, (заведующий кафедрой «Электроника и вычислительная техника», Национальный транспортный университет)

Виталий Гурнак, доктор экономических наук, профессор, (профессор кафедры «Транспортное право и логистика», Национальный транспортный университет)

Алексей Ананченко (магистр, Национальный транспортный университет)

Виталий Ананченко (магистр, Государственный университет телекоммуникаций)

КОМПЛЕКСНОЕ ПРИМЕНЕНИЕ ПРЕДПРИЯТИЯМИ МЕТОДОВ ОБЕСПЕЧЕНИЯ ЭКОНОМИКО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ

В статье освещается роль, значение и специфика комплексного применения методов для информационной безопасности телекоммуникационных сетей общего пользования в отраслях промышленности, торговли, транспорта и связи. Показаны пути взаимодействия корпоративных сетей с телекоммуникационными сетями общего пользования. Проанализированы возможности корпоративной информационной системы «Наука в университетах», разработанной Национальным транспортным университетом и внедренной в практику Министерством образования и науки Украины. Обосновывается, что информационная безопасность, как и защита информации, является задачей комплексной, направленной на обеспечение безопасности и реализуется внедрением различных систем безопасности. В статье сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность: целостность данных – защита от сбоев, ведущих к потере информации, защита от несанкционированного создания и уничтожения данных; конфиденциальность информации; доступность информации для всех авторизованных пользователей. Исследованием установлено, что поддержка информационной безопасности – это комплекс организационных, правовых и инженерно-технологических мероприятий по сохранению, охране и защите жизненно важных интересов субъектов информационной деятельности. Информационная безопасность в условиях информатизации Украины (формирование информационного общества) – это общественные отношения по созданию и поддержанию на осознанном, должном уровне функционирования соответствующей автоматизированной (компьютеризированной) информационной системы.

Ключевые слова: *информационная безопасность, телекоммуникационные сети, корпоративные сети, информатизация, информационная система, защита информации.*

Viktor Danchuk, PhD, Professor,
(Head of the «Electronics and Computer Science», National Transport University)

Vitalii Hurnak, PhD, Professor,
(Professor of «Transport Law and Logistics», National Transport University)

Oleksii Ananchenko
(Post graduate student, National Transport University)

Vitalii Ananchenko
(Post graduate student, State University of Telecommunications)

INTEGRATED SUPPORT METHODS OF ENTERPRISES ECONOMIC AND INFORMATION SECURITY OF TELECOMMUNICATIONS NETWORK

The article highlights the role, importance and specificity of the complex application of methods for information security of public telecommunication networks in the sectors of industry, trade, transport and communications. It shows the ways of interaction between corporate networks and public telecommunication networks. The capabilities of a corporate information system «Science in the universities», which was developed by the National Transport University and introduced by the Ministry of Education and Science of Ukraine, have been analyzed. The article substantiates that information security, as well as information protection is a complex task and is aimed at ensuring the safety and is realized by introduction of various security systems. It identifies three basic principles, which should provide information security: data integrity – protection against failures, leading to loss of information, protection against unauthorized creation and destruction of data; confidentiality of information; accessibility of information for all authorized users. The study founds that support for information security – is a complex of organizational, legal, engineering and technological activities for the conservation, preservation and protection of the vital interests of the subjects of information activities. Information security in conditions of Ukraine informatization (information society formation) – is the public relations about establishing and maintaining the proper level of functioning of the appropriate automated (computerized) information system.

Keywords: *information security, telecommunication networks, corporate networks, informatization, information system, information protection.*

Постановка проблеми. Характерними особливостями сучасного суспільства є нагромадження великих обсягів інформації, швидка зміна поколінь технологій і глобалізація ринків праці, що вимагає потужної інформаційної підтримки персоналу середньої і вищої ланок управління, організації різного типу діяльності. Більшість існуючих інформаційних систем використовуються підприємствами та організаціями для ведення різноманітних баз даних.

При аналізі проблематики, пов'язаної з інформаційною безпекою, треба враховувати специфіку даного аспекту безпеки, що полягає в тому, що інформаційна безпека є складовою частиною інформаційних технологій – області, що розвивається безпрецедентно високими темпами. Тут важливі не стільки окремі рішення, що

знаходяться на сучасному рівні, скільки механізми генерації нових рішень, що дозволяють жити в темпі технічного прогресу і стрімкого розвитку конкуренції.

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення інформаційної безпеки. Слід виходити з того, що треба конструювати надійні системи із залученням ненадійних компонентів (програм). У загальному вигляді це можливо, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом всього життєвого циклу інформаційної системи.

Аналіз останніх досліджень та публікацій. Вагомий внесок у становлення і розвиток ефективних організаційно-економічних механізмів забезпечення інформаційної безпеки внесли українські та російські вчені В. Герасименко, В. Домарєв, Д. Зегжда, Г. Конахович, А. Малюк, С. Петренко, С. Расторгуєв, О. Редькін, Ю. Уфімцев, П. Хорєв, В. Хорошко, В. Шорошев. Значний внесок у розвиток цих проблем належить зарубіжним вченим Н. Вінеру, Д. Сяо, Б. Роукеру, Л. Дж. Хоффману, К. Шеннону. Правова природа захисту телекомунікацій розглядалася у працях українських та зарубіжних авторів, зокрема І. Алєксєєвої, І. Арістової, Г. Атамчука, О. Лєонідова, А. Ракітова, А. Чернова, В. Цветкова, Д. Черешкіна, М. Швець та інших. Крім того питанням розвитку технічних засобів забезпечення безпеки інформаційного простору присвятили останні наукові дослідження І. Анісімов, В. Орлов, Т. Лозова, О. Юдін, Є. Мачуцький, В. Гранатуров, С. Довбня, Т. Тардаскіна, О. Нікітчин.

Довготривалі трагічні події в Донецькій та Луганській областях наочно довели важливість захисту інформаційного простору і особливо різноманітних даних корпоративних інформаційних систем та телекомунікаційних мереж загального користування. З останніх публікацій заслуговують на увагу матеріали в журналі «Бизнес и безопасность» №6 за 2014 рік, зокрема «Інформаційна війна: визначення і базові поняття», «Створення системи технічного захисту шляхом аналізу технічних каналів витоку за допомогою матриць небезпечних факторів», «Конкурентна розвідка і модель загроз безпеки бізнесу в організаціях і установах різних форм власності» тощо. Вартий розгляду збірник матеріалів наукової конференції «Інформаційна безпека України», яка була проведена 12 – 13 березня 2015 року Київським національним університетом імені Тараса Шевченка, де розглядались методи, засоби і заходи забезпечення інформаційної та кібернетичної безпеки, науково-технічні та практичні аспекти розроблення та використання засобів технічного захисту інформації, захист інформації автоматизованих систем, втрати від витоку інформації та інші.

Метою статті є визначення важливості інформаційної безпеки корпоративних мереж і телекомунікаційних мереж загального користування для суб'єктів господарської діяльності.

Виклад основного матеріалу дослідження. Інформація в сучасному суспільстві стає пріоритетним активом та фактором успіху роботи підприємств незалежно від галузі промисловості, торгівлі, транспорту та форми його власності. У зв'язку з ростом конкуренції значно виросла кількість спроб несанкціонованого доступу до інформаційних ресурсів. Технічні засоби, призначені для незаконного проникнення в автоматизовані системи, – це різного роду прилади, обладнання, устаткування тощо, за допомогою яких можливе безпосереднє підключення до автоматизованих систем чи каналів передачі даних, або які здатні шляхом формування сигналів, полів, середовищ створити умови для несанкціонованого доступу до інформації з метою ознайомлення з такою інформацією тих осіб, які не мають права доступу до неї, або з метою впливу на процес обробки інформації та порушення роботи автоматизованих систем, спотворення або знищення інформації чи її носіїв.

Інформаційна безпека, як і захист інформації, завдання комплексне, спрямована на забезпечення безпеки, що реалізується впровадженням системи безпеки. Проблема захисту інформації є багатоплановою та комплексною і охоплює низку важ-

ливих завдань. Проблеми інформаційної безпеки постійно поглиблюються процесами проникнення в усі сфери суспільства технічних засобів обробки і передачі даних і, насамперед, обчислювальних систем та телекомунікаційних мереж. На сьогоднішній день сформульовано три базові принципи, які повинна забезпечувати інформаційна безпека: цілісність даних – захист від збоїв, що ведуть до втрати інформації, а також захист від неавторизованого створення або знищення даних; конфіденційність інформації; доступність інформації для всіх авторизованих користувачів.

При розробці комп'ютерних систем, вихід з ладу або помилки в роботі яких можуть призвести до тяжких наслідків, питання комп'ютерної безпеки стають першочерговими. Відомо багато заходів, спрямованих на забезпечення комп'ютерної безпеки, основними серед них є організаційні, правові і технічні.

Розробками багатьох вітчизняних вчених напрацьовано величезний організаційний, науково-теоретичний та методичний матеріал, запропоновано різноманітні практичні рекомендації щодо розв'язання тих чи інших питань, вирішення прикладних завдань стосовно інформаційної безпеки.

Правове забезпечення захисту комп'ютерної інформації в Україні здійснюють, насамперед, Конституція України, Закон України «Про інформацію», Закон України «Про захист інформації в автоматизованих системах», Кримінальний Кодекс України, а також Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», що регулює безпосередньо відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Існує багато відомчих документів захисту інформації.

Телекомунікаційна галузь завжди була найбільш технологічно розвинутою та динамічним драйвером впровадження інноваційних рішень для забезпечення інформаційної безпеки.

Галузевий стандарт з інформаційної безпеки визначає захист інформації як діяльність, спрямовану на запобігання витоку інформації, несанкціонованих і ненавмисних дій на інформацію. Об'єктивно забезпечення інформаційної безпеки є комплексним завданням, реалізується впровадженням системи безпеки з різними засобами та методами для системного забезпечення захисту інформації.

У сфері інформаційної безпеки в цілому найактуальнішими є три групи проблем:

1. Порушення конфіденційності інформації;
2. Порушення цілісності інформації;
3. Порушення працездатності інформаційно-обчислювальних систем.

Основні завдання інформаційної безпеки:

1. Попередження загроз інформаційній безпеці.
2. Зниження та мінімізація збитків при реалізації загроз і виникненні інцидентів інформаційної безпеки.
3. Надання обґрунтованих гарантій досягнення цілей забезпечення інформаційної безпеки.

Тому важливо убезпечити взаємодію корпоративної мережі з телекомунікаційними мережами загального користування. Захист периметру корпоративної мережі в сучасних умовах залишається одним із обов'язкових методів забезпечення інформаційної безпеки. Захист периметра традиційно потрібен при підключенні корпоративних мереж до телекомунікаційних мереж загального користування. Завдяки цьому захисту можна запобігти атаки на інформаційні ресурси, організувати безпечний доступ персоналу компанії до зовнішніх мереж, а віддалених авторизованих користувачів – до внутрішніх ресурсів.

Захист периметра включає в себе використання таких засобів, як шлюзи безпеки, міжмережеві екрани (Firewalls), віртуальні приватні мережі (VPN), системи виявлення та запобігання вторгнень (IDS/IPS). Але цих методів вже явно недостатньо для повноцінного захисту інформаційного простору. Найближчим часом слід

очікувати зростання попиту на проекти з модернізації систем захисту периметра, пов'язаних як з підвищенням функціональності і використанням технологій нового покоління, так і з переходом на більш високошвидкісні канали, що вимагають більшої продуктивності засобів захисту.

Останнім часом з'явилися певні додаткои засобів захисту та технології управління. Яскравими прикладами є рішення класів Breach Detection Systems и Firewall Management.

Breach Detection Systems – це додаткові рубежі захисту, що дозволяють протидіяти атакам, що використовують уразливість «нульового дня», а також цілеспрямованим атакам (APT). Рішення Breach Detection Systems інтегруються з традиційними засобами захисту периметра і отримують від них файли. Ці файли запускаються в ізольованому середовищі, що емулює робочі станції користувачів, де проводиться їх динамічний і статичний аналіз. Якщо за результатами аналізу файл визнається шкідливим, то система повідомляє про це, і даний файл буде блокуватися ще на периметрі.

Firewall Management – централізовані та уніфіковані засоби управління міжмережевими екранами. До переваг їх використання належать: можливість управління міжмережевими екранами різних виробників з однієї консолі; візуалізація політик, правил та фільтрації на карті мережі; моніторинг та аналіз змін налаштувань (у тому числі вплив цих змін на безпеку периметру та аналіз на предмет надлишковості/оптимальності правил); автоматизація процесу надання доступу на рівні мережі (інтеграція з системами Service Desk).

Планування, впровадження та забезпечення діяльності Security Operations Center (SOC) в його традиційному розумінні – як ситуаційного центру моніторингу та управління інцидентами інформаційної безпеки – є сьогодні одним з актуальних завдань ефективного функціонування корпоративних інформаційних систем (КІС) із складною IT-інфраструктурою. Тут, в сучасних умовах високого динамізму отримання, обробки та реалізації інформації виникає нагальна потреба у централізованому онлайн-моніторингу подій у різноманітних джерел КІС з відображенням у режимі реального часу, кореляції результатів, надання відповідних звітів та попереджень, що дає можливість забезпечити відповідальний персонал та користувачів повною інформацією про її стан і тим самим забезпечити можливість ефективно управляти ризиками системи. Найбільш ефективним підходом для вирішення такого класу задач, на наш погляд, уявляється використання сучасних систем управління інформацією та повідомленнями безпеки (Security Information and Event Management (SIEM)) [1].

Як приклад діючої КІС можна розглянути систему «Наука в університетах», що була розроблена Національним транспортним університетом та впроваджена в Міністерстві освіти і науки України. Ця система призначена для автоматизованого супроводу наукових проектів вищих навчальних закладів та наукових установ на етапах їх формування, проведення конкурсу, експертизи, звітної компанії. Особливістю клієнт-серверної архітектури КІС є реалізація двох типів (веб- та віконного) додатків, кожен з яких має відповідні типи інтерфейсів: користувацький та адміністративний. Відповідно до типу додатка та інтерфейсу КІС «Наука в університетах» забезпечує прозорість та об'єктивність конкурс проектів; он-лайн режим створення проектів для проходження щорічного конкурсного відбору, експертизи проектів та звітів по проектах, звітування по проектах та науковій та науково-технічній діяльності вищих навчальних закладів та наукових установ в цілому; автоматизований (об'єктивний) розподіл експертів для проведення експертизи; автоматизовану підготовку пакету документів засідання секцій для Міністерства освіти і науки України; формування рейтингових показників проектів та їх виконавців; автоматизоване формування тематичних планів та фінансової звітності; підготовку звітних та аналітичних матеріалів.

За основу реалізації запропонованого підходу захисту інформації в корпоративній інформаційній системі «Наука в університетах» був вибраний продукт AlienVault Open Source SIEM (OSSIM) [3], що являє собою повноцінну безкоштовну відкриту SIEM-систему. AlienVault OSSIM забезпечує усю функціональність, яка вимагається для детектування та профілювання атак, і забезпечує всебічну інтелектуальну платформу управління безпекою з набором відповідних інструментальних засобів. Таким чином, в загальному вигляді інформаційна безпека – це суспільні відносини щодо створення і підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, зокрема підприємництва чи транспорту.

Підтримка інформаційної безпеки – це комплекс організаційних, правових та інженерно-технологічних заходів щодо збереження, охорони та захисту життєво важливих інтересів суб'єктів інформаційної діяльності.

Особливість безпеки інформаційної діяльності полягає у запобіганні, протидії та подоланні природних (стихійних), техногенних і соціогенних (антропогенних) загроз, здатних порушити (чи припинити) життєдіяльність конкретного суб'єкта (людини, соціальних спільнот, суспільства, держави, світового співтовариства).

Поняття та сутність інформаційної безпеки в умовах інформатизації України як соціального явища пропонуємо визначити так:

інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства, кіберцивілізації) – це суспільні відносини щодо створення та підтримання на усвідомленому, належному рівні функціонування відповідної автоматизованої (комп'ютеризованої) інформаційної системи (зокрема систем телекомунікацій); комплекс організаційних, правових та інженерно-технологічних (технічних і програмно-математичних) заходів щодо підтримки (охорони, захисту зберігання), запобігання та подолання природних, техногенних та соціогенних загроз, здатних порушити життєдіяльність конкретної соціотехнічної інформаційної системи.

Відповідно, зазначені формулювання можуть адаптуватися до конкретної (спеціальної) сфери суспільних відносин, зокрема підприємницької діяльності та транспорту.

Стабільне функціонування, зростання економічного потенціалу будь-якого підприємства в умовах ринкових відносин багато в чому залежить від рівня інформаційної безпеки. На наш погляд, в сучасних умовах складовою частиною перспективного комплексу заходів повинна стати програма конкретних дій, спрямованих на створення надійної інформаційної безпеки підприємства, фірми чи холдингу.

Висновки і пропозиції. Забезпечення інформаційної безпеки є важливим фактором збереження ділової репутації оператора зв'язку та фактором його успіху на телекомунікаційному ринку. Оскільки в середовищі корпоративної інформаційної безпеки основна увага сьогодні зосереджена на створенні комплексних систем забезпечення інформаційної безпеки, це вимагає використання цілого спектра технічних рішень та методів. Класичними прикладами є засоби антивірусного захисту, міжмережевого екранування, криптографічного захисту, виявлення вторгнень, запобігання витоків інформації, захисту від несанкціонованого доступу, більш інтелектуальні ─ системи класу SIEM, SOC та інші. При цьому, всі вимоги до методів забезпечення інформаційної безпеки потрібно зводити до знаходження компромісу між безпекою, функціональністю бізнес-систем та зручністю їх використання усіма учасниками взаємодіючих суб'єктів.

ЛІТЕРАТУРА

1. Mosaic Security Research. Log Management & Security Information and Event Management (SIEM)// https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management.

2. *Данчук В.Д.* Синергетична корпоративна інформаційна система управління проектами та програмами/ В.Д. Данчук, Ю.С. Лемешко, Т.А. Лемешко// Управління проектами, системний аналіз і логістика: Науковий журнал. – Вип.9. –К. : НТУ, 2012. – С. 51 – 53.

3. AlienVault Open Source SIEM (OSSIM) // http://www.alienvault.com/.

4. Офіційний веб-портал Верховної Ради України [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua.

5. Статистичний бюлетень України: офіц. текст станом на 31 вер. 2013 р. – К. Державна служба статистики України, 2013. – 22 с.

6. Сайт газети «Магістраль» – www.magistral-uz.com.ua.

7. *Гурнак В.М.* Економічна безпека підприємств транспорту як фактор стабільного задоволення попиту в перевезеннях./ Гурнак В.М., Славінська О.С., Ананченко В.Є.// Управління проектами, системний аналіз і логістика. Науковий журнал. – Вип.10. – К.: НТУ, 2012. – С. 410 – 420.

8. *В.М. Гурнак.* Важливість економічної безпеки підприємств галузей транспорту і зв'язку./ В.М. Гурнак, В.Є. Ананченко// Збірник наукових праць Державного економіко-технологічного університету транспорту. Серія «Економіка і управління». – Вип.21. –К. : ДЕТУТ, 2012. – С. 13 – 32.

9. *В.М. Гурнак.* Економіко-технологічні особливості інфокомунікаційних послуг в України./ В.М. Гурнак, В.Є. Ананченко// Збірник наукових праць Державного економіко-технологічного університету транспорту. Серія «Економіка і управління». – Вип.18. –К. : ДЕТУТ, 2011.– С. 185 – 191.

REFERENCES

1. Mosaic Security Research. Log Management & Security Information and Event Management (SIEM). Available at: https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management.

2. Danchuk V.D., Lemeshko Yu.S., Lemeshko T.A. *Synerhetychna korporatyvna informatsiyna systema upravlinnya proektamy ta prohramamy* [Synergetic corporate information management system of projects and programs], *Upravlinnya proektamy, systemnyy analiz i lohistyka: Naukovyy zhurnal.* [Project Management, System Analysis and Logistics: Scientific journal], 2012, issue 9, pp. 51 – 53.

3. AlienVault Open Source SIEM (OSSIM). Available at: http://www.alienvault.com/.

4. *Ofitsiynyy veb-portal Verkhovnoyi Rady Ukrayiny* [Official Web Portal of the Verkhovna Rada of Ukraine]. Available at: http://zakon.rada.gov.ua.

5. *Statystychnyy byuleten' Ukrayiny: ofits. tekst stanom na 31 ver. 2013 r.* [Statistical bulletin of Ukraine: official text on September 31. 2013]. *Derzhavna sluzhba statystyky Ukrayiny* [State Statistics Service of Ukraine]. 2013. – 22 p.

6. *Sayt hazety «Mahistral'«* [Site of the newspaper «Mahistral'«]. Available at: www.magistral-uz.com.ua.

7. Hurnak V.M., Slavins'ka O.S., Ananchenko V.Ye. *Ekonomichna bezpeka pidpryyemstv transportu yak faktor stabil'noho zadovolennya popytu v perevezennyakh* [Economic security of transport enterprises as a factor of sustainable demand satisfaction in transportation]. *Naukovyy zhurnal «Upravlinnya proektamy, systemnyy analiz i lohistyka»* [Scientific journal «Project Management, System Analysis and Logistics»], 2012, issue 10, pp. 410 – 420.

8. Hurnak V.M., Ananchenko V.Ye. *Vazhlyvist' ekonomichnoyi bezpeky pidpryyemstv haluzey transportu i zv'yazku* [The importance of economic security of transport and communication enterprises]. *Zbirnyk naukovykh prats' Derzhavnoho ekonomiko-tekhnolohichnoho universytetu transportu* [Collection of scientific works of the State Economy and Technology University of Transport]. *Seriya «Ekonomika i upravlinnya»* [Series «Economy and Management»], 2012, issue 21, pp. 13 – 32.

9. Hurnak V.M., Ananchenko V.Ye. *Ekonomiko-tekhnolohichni osoblyvosti infokomunikatsiynykh posluh v Ukrayiny* [Economic and technological features of information and communication services in Ukraine]. *Zbirnyk naukovykh prats' Derzhavnoho ekonomiko-tekhnolohichnoho universytetu transportu* [Collection of scientific works of the State Economy and Technology University of Transport]. *Seriya «Ekonomika i upravlinnya»* [Series «Economy and Management»], 2011, issue 18, pp. 185 – 191.